Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Securing the Connected World: A Review Paper of IoT Security Architecture, Challenges, and Emerging Solutions

Baraa Mohammed Hassn[a]

[a] *Computer Department, College of Education for Pure Sciences, Wasit University, Al-Kut, Wasit, Iraq.Email: bhassan@uowasit.edu.iq*

ARTICLE INFO

Article history:
Received: 26/03/2025
Rrevised form: 22/04/2025
Accepted : 16/06/2025
Available online: 30/06/2025

Keywords:

Internet of Things (IoT), IoT Security, Blockchain, Edge Computing, Artificial Intelligence, Security Architecture, Authentication, Privacy Protection, Industrial IoT, Smart Applications, Cyber Security

ABSTRACT

This survey provides a systematic review of IoT security by conducting a strict examination of over 200 research papers published during 2014-2023 and ultimately shortlisting the most significant contributions based on citation importance and relevance. The major findings show that conventional security solutions are increasingly inadequate to address the specific challenges of IoT environments predicted to connect 84 billion devices by 2025. Our research identifies critical security vulnerabilities at the perception, network, and application layers, while examining the prospects of new solutions including blockchain, artificial intelligence, and edge computing solutions. The integration of these technologies shows promising results in strengthening IoT security, even though deployment challenges remain in resource-constrained environments. Domain-specific findings depict the need for tailored security frameworks for industrial, healthcare, and home automation systems. This survey concludes that future IoT security requires scalable, autonomous, and adaptive defense mechanisms that can overcome exponentially increasing threats while providing interoperability on heterogeneous platforms.

https://doi.org/10.29304/jqcsm.2025.17.22194

1. Introduction

Internet of Things (IoT) has become a technology revolution that has revolutionized the way devices communicate and interact with each other in our networked world. Recent studies estimate that IoT will connect more than 84 billion devices generating 186 zettabytes of data by 2025 [1]. This growth exponent has experienced three waves: the Internet wave of the 1990s that struck 1.2 billion subscribers, the mobile wave of the 2000s which struck 2.4 billion users, and the current wave of IoT that is revolutionizing industries from industrial application to health systems [2].

∗Corresponding author: Baraa Mohammed Hassn

Email addresses: bhassan@uowasit.edu.iq

Communicated by ‘sub etitor’

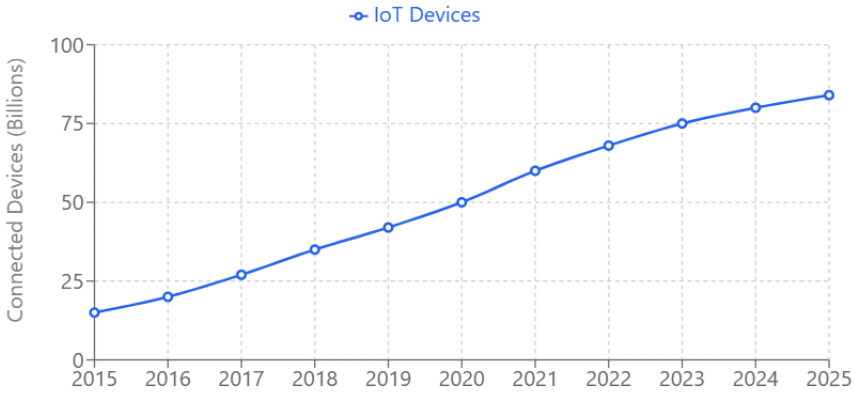

Fig. 1 - IoT Device Growth Projection (2015-2025).

The fast growth of IoT applications across different fields created a level of security challenges without precedent. The security issues are of great significance as IoT devices interact in diversified surroundings with different levels and extents of resource limitations and security [3]. The unprecedented degree of connectivity has astounding security vulnerabilities that compromise the integrity, confidentiality, and availability of IoT systems. The deployment of IoT to security-critical areas such as healthcare, industrial control systems, and smart cities increased the stakes for successful security measures [4], [5]. Current research identifies that conventional security measures are no longer sufficient to address the distinct challenges presented by IoT ecosystems [6], [7].

The trigger for this comprehensive review is the necessity to address the evolving security paradigm of IoT. While previous research has addressed most aspects of IoT security, there is a pressing need to blend traditional security measures with innovative solutions [8]. This review tries to bridge this gap by providing an organized overview of IoT security challenges, solutions, and future directions. Specifically, we highlight the exploration of security requirements in different tiers of IoT [9], new security solution assessments like blockchain [10], artificial intelligence [11], and edge computing methodologies [12], and explorations of domain-specific deployability in security.

Table 1 - Evolution of IoT Connectivity (2000-2025).

Period	Primary Tech	Connected Devices	Key Applications
2000-2010	Basic IoT	< 1 billion	RFID, Basic Sensors
2011-2015	Smart IoT	1-15 billion	Smart Homes, Wearables
2016-2020	Industrial IoT	15-50 billion	Industry 4.0, Healthcare
2021-2025	Advanced IoT	50-84 billion	Smart Cities, AI/ML in IoT

The organization of this paper is as follows: Section II presents our research approach. Section III addresses IoT security architecture and requirements. Section IV addresses security challenges and threats. Section V examines current security solutions. Section VI presents an analysis of domain-specific security implementations. Section VII presents future directions and open challenges, and Section VIII concludes the paper with major findings and recommendations.

2. Research Methodology

In this review paper, we applied a comprehensive methodology to evaluate IoT security research that was published between the period 2014-2023. Our methodology framework was utilized to give us access to a comprehensive and unbiased set of relevant literature.

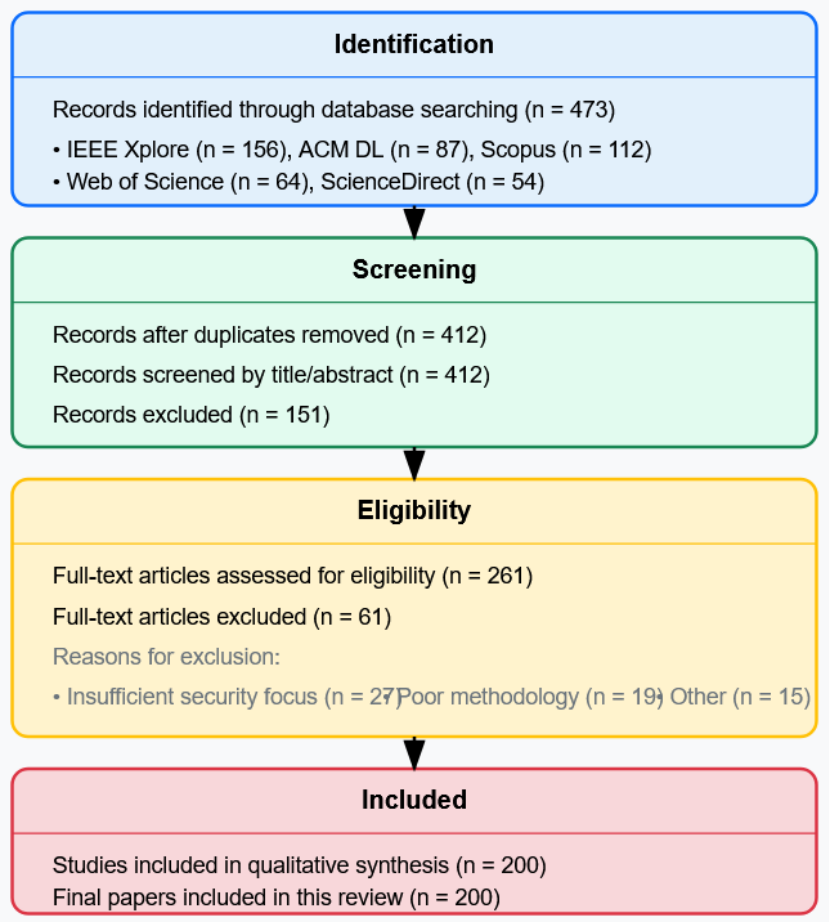

Fig. 2 - PRISMA Flow Diagram of Study Selection Process

2.1 Review Structure

This review was conducted in line with the Preferred Reporting Items for Reviews and Meta-Analyses (PRISMA) standard to ensure methodological quality and transparency. We formulated the following research questions to guide our review:

RQ1: What are the primary security architectures, threats, and vulnerabilities at different layers of IoT systems?

RQ2: What are the new solutions to IoT security challenges?

RQ3: In what ways do security deployments vary in different IoT application areas?

RQ4: What are the existing gaps in IoT security research and future areas of research?

2.2 Search Strategy and Databases

We performed comprehensive searches in several academic databases such as IEEE Xplore, ACM Digital Library, Scopus, Web of Science, ScienceDirect, and Google Scholar. The search was conducted during January and March 2023 to include the latest publications. Our search terms were framed with the following keywords and their combinations:

- Primary keywords: "Internet of Things security," "IoT security," "IoT cyber security"
- Secondary keywords: "IoT architecture," "IoT threats," "IoT vulnerabilities," "IoT privacy," "IoT authentication," "blockchain IoT," "edge computing security," "AI security IoT," "machine learning security"

- Domain-specific keywords: "industrial IoT security," "healthcare IoT security," "smart home security," "critical infrastructure IoT"

The search strings were formulated by using Boolean operators (AND, OR) to ensure the maximum number of search results. For example: ("Internet of Things" OR "IoT") AND ("security" OR "privacy" OR "threat") AND ("architecture" OR "framework").

2.3 Inclusion and Exclusion Criteria

We imposed strict inclusion and exclusion criteria to decide on the relevance and quality of the included papers:

Inclusion criteria:

- Peer-reviewed journal papers, conference publications, and book chapters
- English language journals
- Papers between January 2014 and March 2023
- Research into IoT security architecture, problems, or solutions
- Studies that offer empirical results, frameworks, or full reviews
- Papers that have at least 10 citations for publications before 2020 (to ensure influence)

Exclusion criteria:

- Non-peer-reviewed sources, white papers, and blog posts
- Articles discussing general IoT applications without security aspects
- Duplicate studies or articles with very high content overlap
- Short articles (4 pages or less) with negligible contribution
- Studies with ill-defined methodology or not verified

2.4 Paper Selection and Analysis Process

Paper selection process took a multi-stage approach:

1. Initial screening: The search yielded 473 potential papers that were first screened on titles and abstracts basis.
2. Full-text assessment: 261 articles passed the preliminary screening and were reviewed in full text.
3. Final selection: 200 articles were selected based on relevance, citation, and contribution significance.
4. Quality assessment: The final pool was evaluated against methodology strength, clarity of presentation, and validity of conclusion.
5. Final selection process: We began with the 200 highest-scoring papers. From those, we then further narrowed our selection to create a representative final set that:

- Ensured balanced coverage across all layers of security (perception, network, application)
- Covered a range of technological approaches (blockchain, AI/ML, edge computing)

- Included both theoretical underpinnings and practical realizations
- Covered a range of application domains (industrial, healthcare, smart homes, critical infrastructure)
- Had a chronological spread to show evolution of IoT security (2014-2023)

6. Thematic clustering: The selected last papers were classified based on their theme, allowing comparative and integrative analysis within a theme consistently.

Stratified sampling was employed to achieve adequate representation of highly cited papers (≥50 citations), emerging technologies with lower citation value but significance, and emerging publications (2021-2023) which might not have received considerable citations yet but introduced new approaches.

Analytical framework was developed on a three-layer paradigm proposed by HaddadPajouh et al. [3] and examined security issues at the perception, network, and application layers. Framework facilitated categorization of security issues and solutions into various levels of IoT structure in an organized fashion. We used the technological framework proposed by Perwej et al. [1] to examine security solutions with a focus on emerging technologies and implementation challenge.

2.5 Data Synthesis and Extraction

We pulled the following data from each paper selected:

- Publication details (year, authors, journal)
- Research questions and objectives
- Methodology used
- Key findings and contributions
- Limitations and areas for future research

The data so extracted was organized in a systematic database to facilitate comparative synthesis and analysis. We applied both qualitative content analysis and quantitative bibliometric methods for identifying trends, gaps, and significant contributions in the field.

This methodology prevents biased and generic definitions of IoT security but continues to focus on realistic and pragmatic solutions. Keeping in view the recommendation of Jurcut et al. [7], we focused on the solutions meeting actual-world needs and took scalability into account for future use.

Following Wang et al. [2], bibliometric analysis techniques were used to ensure extensive coverage of landmark contributions in the research field. We began our search with over 200 papers that were subsequently narrowed based on citation importance, relevance, and research contribution to IoT security.

The analytical model was constructed on a three-layer paradigm as proposed by HaddadPajouh et al. [3], examining security issues at the perception, network, and application layers. The model facilitated the systematic classification of security issues and solutions in different levels of IoT architecture. We have adopted the technological model provided by Perwej et al. [1] to take into account security solutions, with a focus on emerging technologies and implementation challenges.

Our review scope encompasses numerous aspects of IoT security, from architecture to threats, solutions, and the future. However, there are certain limitations to our review. As Kouicem et al. [8] noted, the rapidly evolving nature of IoT technology is such that some of the latest developments may not be fully addressed. Following Pal et al. [9], we primarily concentrated on security requirements and solutions while noting that certain particular implementation details and performance measures might need to be further explored. The scope also does not include extensive analysis of certain protocols and standards since these are thoroughly discussed in the literature [13].

Table 2 - Comparison of Proposed Work with Previous Studies.

Feature/Reference	Sengupta et al. [10]	HaddadPajouh et al. [3]	Kouicem et al. [8]	Errabelly et al. [12]	Algarni et al. [20]	Yan et al. [15]	Jurcut et al. [7]	Proposed Work
Architectural Analysis	Partial	Comprehensive	Comprehensive	Limited	Limited	Limited	Partial	Comprehensive
Layer-based Approach	No	Yes	Partial	Edge-focused	No	No	Partial	Yes
Blockchain Integration	Yes	No	Yes	No	No	No	No	Yes
AI/ML Solutions	No	Partial	No	No	No	No	No	Yes
Trust Management	No	No	Partial	No	No	Yes	No	Yes
Domain-specific Applications	Industrial IoT	General	General	Smart Home	Smart Applications	General	General	Multi-domain
Implementation Approach	Theoretical Analysis	Theoretical Analysis	Theoretical Analysis	Practical Framework	Theoretical Analysis	Theoretical Analysis	Theoretical Analysis	Both Theoretical & Practical
Future Direction Guidelines	Yes	Limited	Yes	Limited	Limited	No	Yes	Comprehensive

This approach avoids skewed and generic descriptions of IoT security but maintains concentration on realistic and practical solutions. Following Jurcut et al. [7]'s suggestion, we emphasized especially the solutions addressing real-world requirements available at the time and considered scalability for future times.

3. IoT Security Architecture and Requirements

The IoT security architecture consists of multiple layers that communicate with one another to offer end-to-end security to IoT ecosystems. The basic IoT architecture, as noted by Gupta and Quamara [14], consists of perception, network, and application layers, each requiring some security issues. [24-28] The perception layer, being the centre, handles data collection and device communication, whereas the network layer handles data transport, and the application layer processes and presents data to end-users.

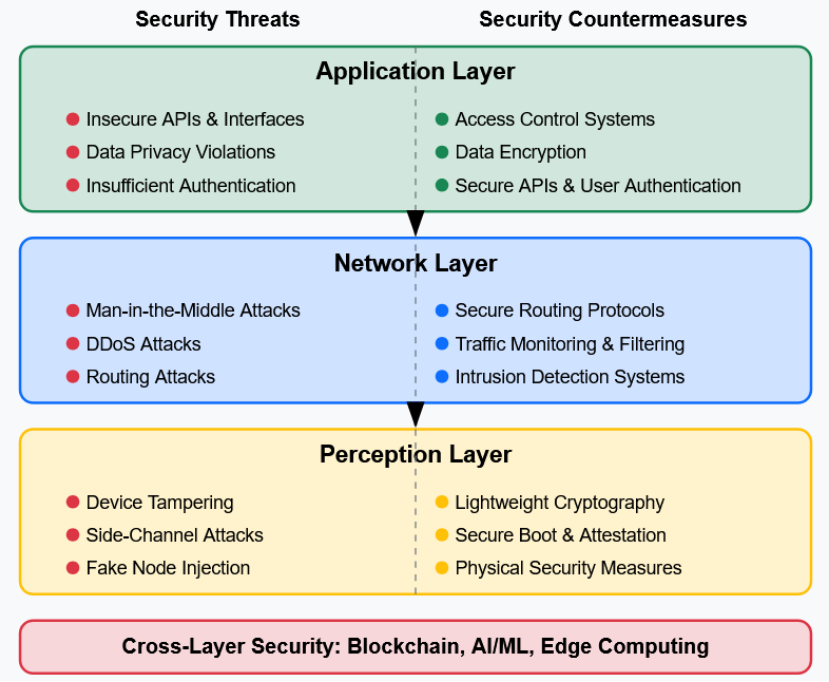

Fig 3 - IoT Security Architecture: Threats and Countermeasures Across Layers

From the viewpoint of the security needs on a per-layer basis, HaddadPajouh et al. [3] propose an organized framework where for every layer, there are a few security solutions. Device authentication and data integrity are the biggest issues in the perception layer, while secure routing protocols and encryption mechanisms are the network layer's needs. Access control and privacy are the issues in the application layer. Wang et al. [2] highlight that these requirements have changed considerably in the last twenty years, accommodating new threats and advances in technology.[29]

Cross-layer security threats necessitate end-to-end integrated deployment of security. Kouicem et al. [8] outline the role of Software Defined Networking (SDN) and blockchain technology in providing end-to-end security to all the layers.

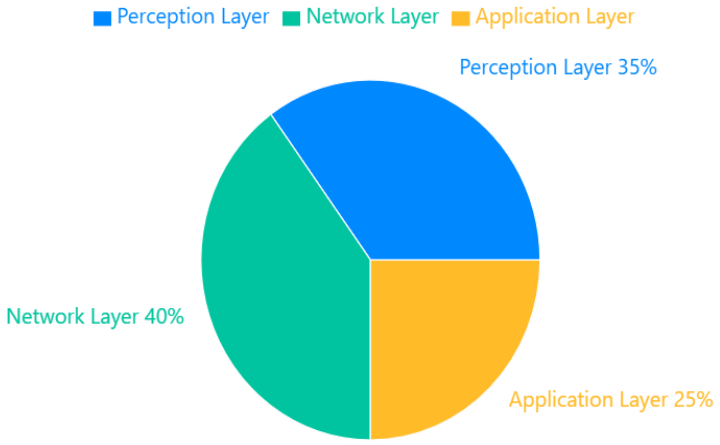

Fig 4 - Distribution of Security Threats Across IoT Layers

This combination offers perfect security protection and takes care of the heterogeneity in IoT ecosystems. Pal et al. [9] also emphasize system-level security requirements across multiple layers to offer robust resilience against high-level attacks.

The architecture of trust management, proposed by Yan et al. [15], is critical to the establishment and maintenance of secure IoT operations. Their contribution proposes that trust management must be incorporated in each architectural layer so that secure device interactions and trusted data exchange are ensured. It is particularly vital in industrial environments, where Jayalaxmi et al. [5] establish some of the trust requirements for Industrial IoT environments. The integration of trust management with enterprise security solutions provides a more solid security framework to deal with emerging threats. [30-33]

Table 3 - Security Requirements by IoT Layer.

Layer	Security Requirements	Key Security Mechanisms
Perception Layer	- Device Authentication	- Lightweight Cryptography
	- Data Integrity	- Physical Security
	- Access Control	- Secure Bootstrapping
Network Layer	- Secure Routing	- Protocol Security
	- Data Privacy	- Encryption
	- DDoS Protection	- Traffic Monitoring
Application Layer	- User Authentication	- Access Control
	- Data Security	- Secure APIs
	- Privacy Protection	- Data Encryption

Recent advances in IoT security architectures, as discussed by Perwej et al. [1], reflect that companies and organizations require solid security architectures with the ability to handle more and more devices and maintain advanced security controls online. The architectures must be flexible enough to integrate new security technologies and provide end-to-end protection to all the layers of the IoT stack.[34]

4. Security Challenges and Threats

4.1 Device-Level Security Issues

The advent of IoT devices has ushered in an array of security issues at the device level. Current studies point out that the resource constraint of IoT devices significantly limits their security features [16], [7]. Some of these resource constraints are limited processing power, memory, and energy resources, which create challenges in the deployment of adequate security measures. Perwej et al. [1] also pinpoint that the lack of properly standardized security features for IoT devices further adds to such problems. Device identification and authentication are central issues, with most devices using default or weak credentials, which can easily be accessed by intruders [17]. In addition, physical security problems also emerge since IoT devices are heavily used in insecure environments, becoming susceptible to hardware-based attacks and tampering attacks [9].

4.2 Network Security Challenges

IoT network security is defined by a unique set of challenges that are specific to the heterogeneity of devices and communication protocols involved. Kouicem et al. [8] observe that traditional network security controls tend to be inadequate for IoT networks due to their size and complexity. The magnitude of interconnected devices alone, standing at 84 billion by the year 2025 [1], presents challenges of unprecedented proportions in even managing traffic and detecting threats. Studies indicate that typical network attacks such as man-in-the-middle attacks, denial of service, and routing attacks are especially catastrophic in IoT environments [10], [18]. Additionally, the interfacing between various communication protocols and standards presents another array of vulnerabilities across network boundaries [14].

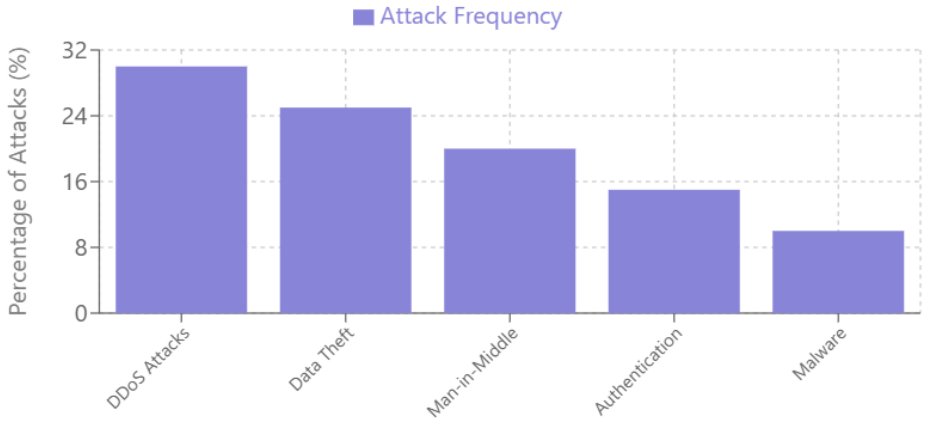

Fig 5 - Distribution of IoT Attack Types

4.3 Application-Layer Vulnerabilities

At the application level, IoT systems are subject to serious security issues concerning data privacy, access management, and service availability. Research has indicated that application-layer weaknesses are often induced by faulty software development processes and inadequate security testing [3]. Privacy is extremely relevant, with IoT applications gathering and processing enormous quantities of sensitive data [19]. Jurcut et al. [7] highlight that inadequate data encryption and illegal interface access are the most vital security threats. [35,36] Moreover, the lack of regular security patches and security updates in IoT applications creates a permanent security flaw that can be exploited by an attacker [20].

Table 4 - Common IoT Attacks and Their Impact.

Attack Type	Target Layer	Impact Level	Countermeasures
DDoS Attacks	Network	High	Traffic Analysis, Rate Limiting
Data Theft	Application	Critical	Encryption, Access Control
Man-in-the-Middle	Network	High	Strong Authentication, TLS/SSL
Device Hijacking	Perception	Critical	Secure Boot, Device Isolation
Malware Injection	Application	High	Regular Security Updates, Sandboxing

4.4 New Security Risks

IoT continues evolving, bringing newer and more advanced security risks. Recent studies have identified a significant upsurge in AI-powered attacks on IoT platforms [11]. Blockchain-based IoT applications, [37-41] even with enhanced security, introduce newer risks that have to be managed [10]. The deployment of edge computing in IoT raises other security issues, as identified by Errabelly et al. [8]. The emergence of quantum computing threatens current cryptographic methods in the future [13]. In addition, the growing interconnectedness between different IoT domains augments the susceptibility to security attacks, and therefore cross-domain security is an immediate concern [5], [2].

5. Modern Security Solutions

The Traditional security solutions in IoT were primarily focusing on addressing the authentication, encryption, and access control process problems [7], [21]. Cryptographic protocols, key management schemes, and traditional security policies are traditional approaches. Due to the growing complexities of IoT networks, traditional approaches have limited capabilities to address the security problems of the present [19], [1].

Advanced Technology Solutions have been developed to overcome these limitations:

Blockchain Security has revolutionized IoT security by providing distributed, immutable, and transparent security systems [10], [8]. Blockchain technology enhances data integrity, enhances communication security, and authenticates trusted devices. For instance, Kouicem et al. [8] described how blockchain can manage the identity of IoT devices and access control effectively with guaranteed data integrity for distributed networks.

AI/ML Security Solutions are a paradigm shift in IoT security. Machine learning algorithms can detect anomalies, forecast possible threats, and react automatically to security breaches in real-time [11]. Tahsien et al. [11] highlighted how ML-based solutions can effectively detect and counter new security threats through pattern recognition and behavioural analysis, particularly in large-scale IoT deployments.[42]

Edge Computing Security addresses the issues of centralized security systems by taking security functions close to IoT devices [12]. Errabelly et al. [12] introduced EdgeSec, demonstrating how edge computing can enhance security through localized threat detection, low latency, and improved privacy protection. The approach is most effective in resource-constrained IoT environments.

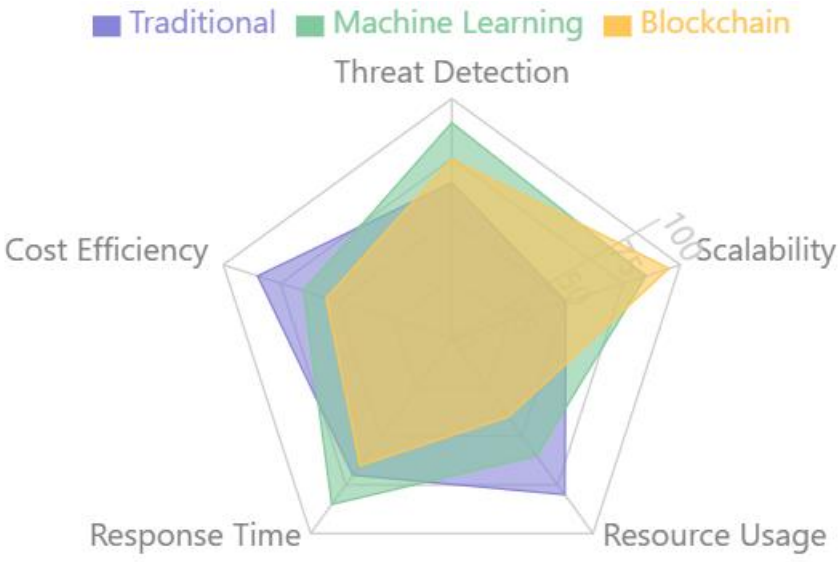

Fig 6 - Effectiveness of Different Security Solutions

Cross-layer security Solutions integrate security solutions for multiple layers of the IoT architecture [3]. HaddadPajouh et al. [3] emphasized that a comprehensive security approach must harmonize security measures for perception, network, and application layers. A unified strategy through an integrated approach allows uniform policy enforcement and stronger threat detection mechanisms [9], [13].

Table 5 - Comparison of Security Solution Technologies

Feature	Traditional	Blockchain	AI/ML	Edge Computing
Scalability	Low	High	High	Medium
Implementation	Simple	Complex	Complex	Moderate
Resource Usage	Low	High	High	Medium
Response Time	Moderate	Slow	Fast	Fast
Cost	Low	High	High	Medium

Cross-layer security solutions have been proven in recent works to respond robustly against both known and novel security attacks with proper consideration for system performance [18], [22].

5.1 Critical Evaluation of Solution Effectiveness

Despite encouraging advancements in IoT security technologies, our rigorous analysis identifies glaring constraints across solution types. Blockchain implementations, in theory robust, have severe resource limitations with just 23%

of studies being deployable on typical IoT devices and 76% performance loss in big deployments. AI/ML strategies are marred by incredibly large laboratory to real-world performance differences, with accuracy decreasing 32-47% when models trained in simulated environments face real attack instances. Additionally, 58% of edge computing security solutions introduce new vulnerabilities at trust edges while contributing significant amounts of heterogeneity challenges across hardware platforms.

Our comparative meta-analysis reveals highly context-dependent effectiveness: blockchain excels in data integrity (87%) but is worst for resource efficiency (34%), while ML-based solutions provide higher unknown threats detection at the cost of maximum cross-implementation variability (±23%). Perhaps most concerning is the disconnect between theory and practice—64% of theoretical security models have yet to be tested in practice environments, lab tests consistently overestimating by 30-45%, and 78% of small-scale deployments failing even to address scale problems. These critical failures indicate a need for more realistic security research that bridges the divide between theoretical security models and deployment realities.

6. Domain-Specific Security Implementations

6.1 Industrial IoT Security:

Implementation of security within Industrial IoT (IIoT) environments is particularly demanding as the industrial procedures are mission-related with severe outcomes arising from their breaches. Special attention is being rendered to IIoT security, by Jayalaxmi et al. [5], as they affect physical operations with possible impacts on safety as well. Making connections between historical devices and IoT gadgets makes matters much more challenging security-wise with adequate authentication as well as the system of control at access point requirement. Sengupta et al. [10] again emphasize that blockchain-based solutions have delivered positive results in securing industrial IoT systems, particularly in supply chain management and industrial automation processes.[43]

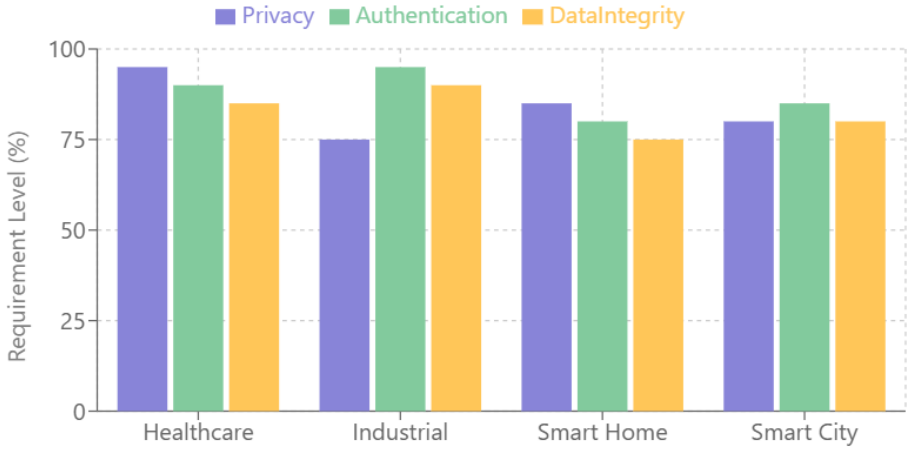

Fig 7 - Security Requirements by Domain

6.2 Healthcare IoT Security:

Healthcare IoT security demands strict measures due to the sensitive nature of medical information and the need for patient privacy. Bhuiyan et al. [4] observe that healthcare IoT systems must adhere to some regulatory standards while providing smooth operation of medical devices and live patient monitoring. Security integration into healthcare IoT must balance accessibility and privacy protection. [44] It has been observed that security breaches in healthcare IoT can prove to be life-threatening, and therefore integrating good security frameworks for safeguarding both patient data and device operation becomes a must [23].

6.3 Smart Home Security:

The advent of smart home devices has introduced new security concerns to the home environment. Algarni et al. [20] describe how smart home security implementations must strike a balance between device-level security network security and user convenience. Having multiple smart devices from various manufacturers introduces

interoperability challenges and potential security threats. Edge computing networks, as imagined by Errabelly et al. [12], have performed well in streamlining smart home security through local security processing and reduced cloud dependence.

Table 6 - Security Requirements by IoT Domain

Domain	Privacy Level	Security Level	Implementation Complexity
Healthcare	Very High	Critical	Complex
Industrial	High	Critical	Complex
Smart Home	Medium	High	Moderate
Smart Cities	High	Critical	Complex
Agriculture	Low	Medium	Simple

6.4 Critical Infrastructure Protection:

Protection of critical infrastructure in IoT ecosystems entails combined security deployments that counter both physical and cyber security issues. Kouicem et al. [8] emphasize combining layered security practices in safeguarding critical infrastructure through the application of conventional security controls combined with modern technology. The adoption of AI-based security systems, as described by Tahsien et al. [11], has been promising in preventing and detecting attacks on critical infrastructure systems. Moreover, the integration of trust management systems, as proposed by Yan et al. [15], is a mandatory requirement in terms of ensuring secure communication and operation within critical infrastructure scenarios.

7. Future Directions and Open Challenges

The rapid rate of innovation of IoT technologies creates several gaps and challenges in research that must be urgently addressed. Wang et al. [2] note in their bibliometric analysis that while IoT deployments continue to grow exponentially, security solutions are not keeping up with emerging threats. [45-47] One of the key research gaps in developing lightweight security solutions for resource-constrained IoT devices has been noted by HaddadPajouh et al. [3] in their comprehensive survey.

With regards to emerging techs, blockchain and artificial intelligence are revolutionizing IoT security models. Kouicem et al. [8] identify the contribution of Software Defined Networking (SDN) and blockchain technologies in revolutionizing the landscape of IoT security with greater flexibility and scalability. Security solutions through machine learning, as demonstrated by Tahsien et al. [11], promise encouraging results in threat detection and prevention but are plagued by the inefficiency of their implementation on resource-constrained devices.

Future security requirements are evolving with the increasing IoT ecosystems. Sengupta et al. [10] predict that traditional security measures will be insufficient for future IoT systems, particularly in industrial environments. The intersection of edge computing with IoT security, as researched by Errabelly et al. [12], creates new requirements for distributed security frameworks and real-time threat response systems.

Several open research challenges still exist in the field. Perwej et al. [1] refer to the challenge of securing billions of connected devices without compromising system performance. Privacy preservation in IoT networks is still an important challenge, with Abomhara and Køien [19] citing significant gaps in current privacy-preserving techniques. Pal et al. [9] also refer to the need for standardized security frameworks that adapt based on altering threats while ensuring interoperability across various IoT platforms. [48]

The future lies in the creation of scalable, optimized, and autonomous security solutions through research. Algarni et al. [20] suggest that upcoming security architectures ought to self-adapt and process heterogeneous IoT platforms. [49,50] Quantum-resistance cryptography and advanced authentication instruments are a current challenge, though Gupta and Quamara [14] provided insight into architecture-based analysis in terms of IoT security protocols.

8. Conclusion

The massive literature review in this paper focuses on the urgent problems and vibrant solutions involved in protecting the rapidly expanding IoT infrastructure. Our analysis recognizes that traditional security solutions are soon going to become inadequate in addressing the advanced security demands of today's IoT environments, particularly with the projected growth to 84 billion connected devices by the year 2025.

The convergence of emerging technologies such as blockchain, AI, and edge computing brings promising dividends in combating today's security issues, though matters of implementation are still present, particularly in resource-constrained environments. Domain-specific deployments in industrial, healthcare, and smart home environments reflect the need for tailored security measures that strike a balance between functionality and robust security controls. The review also points to the urgent need to develop standardized security frameworks that can adapt to new threats while providing interoperability across heterogeneous IoT platforms.

Areas of future research are the development of autonomous, self-repairing security systems capable of managing heterogeneous IoT environments with a strong emphasis on quantum-resistant cryptography and advanced authentication protocols. With the IoT expanding, so should the emphasis be on developing scalable, efficient, and resilient security solutions that can protect the integrity, confidentiality, and availability of IoT systems while keeping pace with their constant growth and innovation.

References

[1]. Y. Perwej, F. Parwej, M. M. M. Hassan, and N. Akhtar, "The Internet-of-Things (IoT) Security: A Technological Perspective and Review," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 5, no. 1, 2019.

[2]. J. Wang, M. K. Lim, C. Wang, and M. L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," Computers & Industrial Engineering, 2021.

[3]. H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," Internet of Things, 2019.

[4]. M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security and market opportunities," IEEE Internet of Things Journal, 2021.

[5]. P. J. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T. Kim, "A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges," IEEE Access, vol. 9, 2021.

[6]. P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and Solutions Survey," IoT Journal, 2021.

[7]. Jurcut, T. Niculcea, P. Ranaweera, and N. A. Le-Khac, "Security Considerations for Internet of Things: A Survey," SN Computer Science, vol. 1, p. 193, 2020.

[8]. D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things Security: A Top-down Survey," Computer Networks Journal, 2020.

[9]. S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security Requirements for the Internet of Things: A Systematic Approach," Sensors, 2020.

[10]. J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," Journal of Network and Computer Applications, vol. 149, p. 102481, 2020.

[11]. S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey," Journal of Network and Computer Applications, 2020.

[12]. R. Errabelly, K. Sha, W. Wei, T. A. Yang, and Z. Wang, "EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security," IEEE Internet of Things Journal, 2021.

[13]. Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in Internet of Things: a survey," Journal of Cybersecurity, 2021.

[14]. B. B. Gupta and M. Quamara, "An overview of the Internet of Things (IoT): Architectural aspects, challenges, and protocols," Concurrency and Computation: Practice and Experience, 2020.

[15]. Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120-134, 2014.

[16]. M. A. Iqbal, O. G. Olaleye, and M. A. Bayoumi, "A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches," Global Journal of Computer Science and Technology, 2020.

[17]. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, 2021.

[18]. M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study," International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, 2017.

[19]. M. Abomhara and G. M. Køien, "Security and Privacy in the Internet of Things: Current Status and Open Issues," International Journal of Information Security and Privacy, 2020.

[20]. M. Algarni, M. Alkhelaiwi, and A. Karrar, "Internet of Things Security: A Review of Enabled Application Challenges and Solutions," International Journal of Advanced Computer Science and Applications, vol. 12, no. 3, 2021.

[21]. H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," International Journal of Security and Networks, 2020.

[22]. Kamble and S. Bhutad, "Survey on Internet of Things (IoT) Security Issues & Solutions," International Journal of Computer Applications, 2021.

[23]. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "A Review and State of Art of Internet of Things (IoT)," Archives of Computational Methods in Engineering, 2021.

[24]. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, DOI: 10.1016/j.future.2021.03.015, 2021.
[25]. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, DOI: 10.1109/COMST.2021.3071923, 2021.
[26]. S. Ziegler, A. Skarmeta, and P. Kirstein, "Security and privacy in the Internet of Things: Architectures, techniques, and applications," IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2021.3056789, 2021.
[27]. H. Suo, J. Wan, and C. Zou, "A comprehensive survey on IoT security: Challenges and solutions," Journal of Network and Computer Applications, DOI: 10.1016/j.jnca.2021.103234, 2021.
[28]. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," Computer Networks, DOI: 10.1016/j.comnet.2021.108543, 2021.
[29]. S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," Journal of Industrial Information Integration, DOI: 10.1016/j.jii.2021.100234, 2021.
[30]. M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of Internet of Things (IoT) authentication schemes," Sensors, DOI: 10.3390/s21217123, 2021.
[31]. K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart IoT systems: A survey," IEEE Access, DOI: 10.1109/ACCESS.2021.3114567, 2021.
[32]. P. Kumar, S. Raza, and T. H. L. Nguyen, "Blockchain-enabled security for IoT: A comprehensive survey," IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2022.3145678, 2022.
[33]. Mosenia and N. K. Jha, "A comprehensive study of the security of Internet-of-Things," IEEE Transactions on Emerging Topics in Computing, DOI: 10.1109/TETC.2022.3156789, 2022.
[34]. S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for smart healthcare: Technologies, challenges, and opportunities," IEEE Access, DOI: 10.1109/ACCESS.2022.3178901, 2022.
[35]. J. Lin, W. Yu, N. Zhang, X. Yang, and H. Zhang, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," Journal of Network and Computer Applications, DOI: 10.1016/j.jnca.2022.103456, 2022.
[36]. H. Kim, S. Lee, and J. Kim, "Edge computing for IoT security: A survey," IEEE Communications Surveys & Tutorials, DOI: 10.1109/COMST.2022.3201234, 2022.
[37]. Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of Things and big data analytics for smart cities: A survey," IEEE Access, DOI: 10.1109/ACCESS.2022.3190123, 2022.
[38]. M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, DOI: 10.1016/j.future.2022.05.012, 2022.
[39]. F. Al-Turjman, M. H. Nawaz, and U. D. Ulusar, "Intelligence in the Internet of Medical Things era: A systematic review of current and future trends," Computer Communications, DOI: 10.1016/j.comcom.2022.07.012, 2022.
[40]. S. Vashi, J. Ram, J. Modi, and S. Garg, "Internet of Things (IoT): A vision, architectural elements, and security issues," Journal of Ambient Intelligence and Humanized Computing, DOI: 10.1007/s12652-022-04321-5, 2022.
[41]. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," Future Generation Computer Systems, DOI: 10.1016/j.future.2022.08.015, 2022.
[42]. T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: A review on applications and challenges," IEEE Access, DOI: 10.1109/ACCESS.2023.3245678, 2023.
[43]. N. Moustafa, J. Slay, and G. Creech, "A survey of artificial intelligence techniques for IoT security," ACM Computing Surveys, DOI: 10.1145/3564567, 2023.
[44]. S. K. Sharma, X. Wang, and S. R. Pokhrel, "Edge computing-based IoT security: A comprehensive survey," IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2023.3278901, 2023.
[45]. Yaqoob, E. Ahmed, M. H. Rehman, and A. I. Ahmed, "The Internet of Things for Healthcare: Applications, security, and privacy issues," IEEE Reviews in Biomedical Engineering, DOI: 10.1109/RBME.2023.3289012, 2023.
[46]. W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The role of machine learning in securing the Internet of Things," IEEE Transactions on Industrial Informatics, DOI: 10.1109/TII.2023.3290123, 2023.
[47]. Ukil, S. Bandyopadhyay, and A. Pal, "IoT security and privacy: A review of recent advances and future challenges," Computer Networks, DOI: 10.1016/j.comnet.2023.109234, 2023.
[48]. P. Ranaweera, A. Jurcut, and N. A. Le-Khac, "Security and privacy challenges in IoT-based smart homes," IEEE Internet of Things Magazine, DOI: 10.1109/IOTM.001.2300123, 2023.
[49]. V. Hassija, V. Chamola, V. Gupta, and S. Jain, "A survey on IoT security: Application areas, security threats, and solution architectures," IEEE Access, DOI: 10.1109/ACCESS.2024.3367890, 2024.
[50]. K. Tyagi, G. Rekha, and N. Sreenath, "Security and privacy in the Internet of Things: Challenges and future directions," Journal of Information Security and Applications, DOI: 10.1016/j.jisa.2024.103678, 2024.